ÁLGEBRA **Examen de septiembre** **3-9-2003**

Apellidos **Nombre**

Ejercicio 1. (*2,5 puntos*) Sea $\mathbb{F}_2 = \mathbb{Z}/\mathbb{Z}2$ el cuerpo finito con dos elementos. Sea α raíz de X^2+X+1 sobre $\mathbb{F}_2$ y $K_1 = \mathbb{F}_2[\alpha]$. Sea $g(X) = X^2 + \alpha X + 1 \in K_1[X]$.

1. ¿Cuántos elementos tiene K_1? Expréselos en función de α.
2. Pruebe que $g(X)$ es irreducible sobre $K_1[X]$.
3. Sea β raíz de $g(X)$ y $K_2 = K_1[\beta]$. ¿Cuántos elementos tiene K_2? Calcule $[K_2 : \mathbb{F}_2]$.
4. Sea $\varphi : K_2 \to K_2$ definida por $\varphi(x) = x^2$. Pruebe que $\varphi \in \mathrm{Gal}(K_2|\mathbb{F}_2)$, y que el orden de φ es 4. Deduzca que $\mathrm{Gal}(K_2|\mathbb{F}_2) = \langle\varphi\rangle$.

Solución.

1. El polinomio $X^2 + X + 1$ es el polinomio mínimo de α sobre $\mathbb{F}_2$. entonces, los elementos de K_1 son de la forma $a_0 + a_1\alpha$, con $a_0, a_1 \in \mathbb{F}_2$. Entonces K_1 tiene 4 elementos, que son $0, 1, \alpha, 1 + \alpha$.
2. Como $g(X)$ es de grado 2, basta ver que ningún elemento de K_1 es raíz de $g(X)$. Es una mera comprobación que $g(0), g(1), g(\alpha), g(1 + \alpha) \neq 0$.
3. Com en el primer apartado, los elementos de K_2 son de la forma $b_0 + b_1\beta$, con $b_0, b_1 \in K_1$. Como hay 4 posibilidades para b_0 y b_1, tenemos que K_2 tiene $2^4 = 16$ elementos. Se sigue que $[K_2 : \mathbb{F}_2] = 4$, o bien, como $[K_2 : K_1] = 2, [K_1 : \mathbb{F}_2] = 2$ entonces $[K_2 : \mathbb{F}_2] = 4$.
4. La aplicación φ no es más que el automorfismo de Frobenius de K_2, explicado en teoría. Por tanto, $\varphi \in \mathrm{Gal}(K_2|\mathbb{F}_2)$ y es generador del grupo. Como $|\,\mathrm{Gal}(K_2|\mathbb{F}_2)| = [K_2 : \mathbb{F}_2] = 4$, tenemos que su orden es 4.

   En cualquier caso, se puede probar directamente. Veamos que es un endomorfismo inyectivo de cuerpos. Es claro que $\varphi(ab) = (ab)^2 = a^2b^2 = \varphi(a)\varphi(b)$. Por otro lado,

   $$\varphi(a + b) = a^2 + 2ab + b^2 = a^2 + b^2 = \varphi(a) + \varphi(b).$$

   El carácter inyectivo es inmediato. Como K_2 es finito, entonces φ tiene que ser sobreyectivo, esto es, automorfismo. Además, si $a \in \mathbb{F}_2$, entonces $a^2 = a$, por lo que $\varphi \in \mathrm{Gal}(K_2|\mathbb{F}_2)$. Como el orden de φ tiene que dividir al orden de $\mathrm{Gal}(K_2|\mathbb{F}_2)$, que es 4, basta ver que φ^2 no es la identidad. Por ejemplo, se puede comprobar que $\varphi^2(\beta) \neq \beta$.

Ejercicio 2. (*3 puntos*) Sea $f(X) = X^8 - 1 \in \mathbb{Q}[X]$ y α una raíz octava primitiva de la unidad, por ejemplo $\alpha = \frac{1}{2}(1 + i)\sqrt{2}$. Sea K un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$ y G el grupo de Galois de $f(X)$ sobre $\mathbb{Q}$.

1. Demuestre que $K = \mathbb{Q}[\alpha]$.
2. Halle $[K : \mathbb{Q}]$.
3. Sea $\sigma \in G$. Pruebe que $\sigma(\alpha) = \alpha^k$ si y solamente si k es impar. Verifique si $\sigma^2 = id$.
4. Si llamamos $x_k = \alpha^k, k = 1, \ldots, 8$ a las raíces de $f(X)$, exprese G como subgrupo de S_8.
5. Halle todos los subgrupos de G.

6. Razone cuáles de los siguientes cuerpos son intermedios entre $\mathbb{Q}$ y K y justifique si hay alguno más:

$$\text{(a) } \mathbb{Q}[i], \quad \text{(b) } \mathbb{Q}[\sqrt{2}], \quad \text{(c) } \mathbb{Q}[\sqrt{-2}], \quad \text{(d) } \mathbb{Q}[\alpha^2], \text{(e) } \mathbb{Q}[\alpha+\alpha^2], \quad \text{(f) } \mathbb{Q}[\sqrt{3}]$$

Solución.

1. Las raíces del polinomio $f(X)$ son $\alpha, \alpha^2, \dots, \alpha^7, \alpha^8 = 1$, por lo que $K = \mathbb{Q}[\alpha, \alpha^2, \dots, \alpha^7] = \mathbb{Q}[\alpha]$.

2. Sabemos que $[K : \mathbb{Q}]$ es el grado del polinomio mínimo de α sobre $\mathbb{Q}$. Es un divisor de $X^8 - 1 = (X^4 - 1)(X^4 + 1)$. Como $\alpha^4 - 1 \neq 0$, se tiene que α es raíz de $g(X) = X^4 + 1$. Se trata de probar que $g(X)$ es irreducible sobre $\mathbb{Q}[X]$. Si $g(X) = g_1(X)g_2(X)$, con $g_1(X), g_2(X) \in \mathbb{Q}[X]$, no puede ocurrir que $g_1(X)$ o $g_2(X)$ tenga grado igual a 1, porque esto implicaría que $g(X)$ tiene raíces racionales. Los únicos candidatos a serlo son 1 y -1, y vemos fácilmente que no lo son. Por tanto, la única posibilidad es que $g_1(X)$ y $g_2(X)$ tengan grado igual a 2. Escribamos

$$g(X) = (X^2 + aX + b)(X^2 + cX + d),$$

con $a, b, c, d \in \mathbb{Q}$. Igualamos coeficientes y nos queda

$$\begin{aligned} 0 &= a + c, \\ 0 &= b + d + ac, \\ 0 &= ad + bc, \\ 1 &= bd. \end{aligned}$$

De la cuarta deducimos que $b \neq 0$ y que $d = \frac{1}{b}$. De la primera tenemos que $c = -a$, y con la segunda llegamos a $0 = b + \frac{1}{b} - a^2$. La tercera, entonces, nos da $0 = a(\frac{1}{b} - b)$. Las posibilidades son

- $a = 0$, de donde $b + \frac{1}{b} = 0$, pero $b \in \mathbb{Q}$.
- $b = \frac{1}{b}$, lo que implica que $b = \pm 1$, pero entonces se tiene que $0 = -2 - a^2$ o bien $0 = 2 - a^2$, incompatible con $a \in \mathbb{Q}$.

Luego $g(X)$ es irreducible sobre $\mathbb{Q}[X]$, y entonces $[K : \mathbb{Q}] = 4$.

3. Sea $\sigma \in G$. Como $\alpha^8 - 1 = 0$ tenemos que $\sigma(\alpha)^8 - 1 = 0$, por lo que $\sigma(\alpha) = \alpha^j$ para algún $j = 1, 2, \dots, 8$ (raíces se aplican en raíces). Además, $\alpha^4 + 1 = 0$ y, por el mismo motivo, $\sigma(\alpha)^4 + 1 = 0$. Si $\sigma(\alpha) = \alpha^{2l}$, entonces $0 = (\alpha^{2l})^4 + 1 = (\alpha^8)^l + 1 = 1 + 1$, lo que es absurdo. Por tanto, $\sigma(\alpha)$ tiene que ser una potencia impar de α.

Por el apartado anterior, $|G| = 4$, de donde $\sigma(\alpha)$ solamente puede valer $\alpha, \alpha^3, \alpha^5, \alpha^7$.

Además,

$$\begin{array}{lll} \text{Si } \sigma(\alpha) = \alpha & \Rightarrow \sigma = id & \Rightarrow \sigma^2 = id. \\ \text{Si } \sigma(\alpha) = \alpha^3 & \Rightarrow \sigma^2(\alpha) = (\alpha^3)^3 = \alpha^8\alpha = \alpha & \Rightarrow \sigma^2 = id. \\ \text{Si } \sigma(\alpha) = \alpha^5 & \Rightarrow \sigma^2(\alpha) = (\alpha^5)^5 = (\alpha^8)^3\alpha = \alpha & \Rightarrow \sigma^2 = id. \\ \text{Si } \sigma(\alpha) = \alpha^7 & \Rightarrow \sigma^2(\alpha) = (\alpha^7)^7 = (\alpha^8)^6\alpha = \alpha & \Rightarrow \sigma^2 = id. \end{array}$$

4. Llamemos $x_1 = \alpha, x_2 = \alpha^2, \dots, x_7 = \alpha^7, x_8 = \alpha^8 = 1$.

- Si $\sigma_1(\alpha) = \alpha$ entonces $\sigma_1 = id$.
- Si $\sigma_2(\alpha) = \alpha^3$, entonces

$$\begin{aligned} &\sigma_2(x_1) = x_3, \\ &\sigma_2(x_2) = \sigma_2(\alpha^2) = (\alpha^3)^2 = \alpha^6 = x_6, \\ &\sigma_2(x_3) = \sigma_2(\alpha^3) = (\alpha^3)^3 = \alpha^9 = x_1, \\ &\sigma_2(x_4) = \sigma_2(\alpha^4) = (\alpha^3)^4 = \alpha^4 = x_4, \\ &\sigma_2(x_5) = \sigma_2(\alpha^5) = (\alpha^3)^5 = \alpha^7 = x_7, \\ &\sigma_2(x_6) = \sigma_2(\alpha^6) = (\alpha^3)^6 = \alpha^2 = x_2, \\ &\sigma_2(x_7) = \sigma_2(\alpha^7) = (\alpha^3)^7 = \alpha^5 = x_5, \\ &\sigma_2(x_8) = \sigma_2(1) = 1 = x_8. \end{aligned}$$

de donde identificamos σ_2 con la permutación $(13)(26)(57)$.

- Si $\sigma_3(\alpha) = \alpha^5$, entonces

$$\begin{aligned}
&\sigma_3(x_1) = x_5, \\
&\sigma_3(x_2) = \sigma_3(\alpha^2) = (\alpha^5)^2 = \alpha^2 = x_2, \\
&\sigma_3(x_3) = \sigma_3(\alpha^3) = (\alpha^5)^3 = \alpha^7 = x_7, \\
&\sigma_3(x_4) = \sigma_3(\alpha^4) = (\alpha^5)^4 = \alpha^4 = x_4, \\
&\sigma_3(x_5) = \sigma_3(\alpha^5) = (\alpha^5)^5 = \alpha^1 = x_1, \\
&\sigma_3(x_6) = \sigma_3(\alpha^6) = (\alpha^5)^6 = \alpha^6 = x_6, \\
&\sigma_3(x_7) = \sigma_3(\alpha^7) = (\alpha^5)^7 = \alpha^3 = x_3, \\
&\sigma_3(x_8) = \sigma_3(1) = 1 = x_8.
\end{aligned}$$

de donde identificamos σ_3 con la permutación $(15)(37)$.

- Si $\sigma_4(\alpha) = \alpha^7$, entonces

$$\begin{aligned}
&\sigma_4(x_1) = x_7, \\
&\sigma_4(x_2) = \sigma_4(\alpha^2) = (\alpha^7)^2 = \alpha^6 = x_6, \\
&\sigma_4(x_3) = \sigma_4(\alpha^3) = (\alpha^7)^3 = \alpha^5 = x_5, \\
&\sigma_4(x_4) = \sigma_4(\alpha^4) = (\alpha^7)^4 = \alpha^4 = x_4, \\
&\sigma_4(x_5) = \sigma_4(\alpha^5) = (\alpha^7)^5 = \alpha^3 = x_3, \\
&\sigma_4(x_6) = \sigma_4(\alpha^6) = (\alpha^7)^6 = \alpha^2 = x_2, \\
&\sigma_4(x_7) = \sigma_4(\alpha^7) = (\alpha^7)^7 = \alpha^1 = x_1, \\
&\sigma_4(x_8) = \sigma_4(1) = 1 = x_8.
\end{aligned}$$

de donde identificamos σ_4 con la permutación $(17)(26)(35)$.

Luego $G = \{id, (13)(26)(57), (15)(37), (17)(26)(35)\}$.

5. Como $|G| = 4$ sus subgrupos propios solamente pueden ser de orden 2. Como todos los elementos de G son de orden 2 (apartado 3), tenemos en total los subgrupos

$$H_0 = id, H_1 = G, H_2 = \{id, \sigma_2\}, H_3 = \{id, \sigma_3\}, H_4 = \{id, \sigma_4\}.$$

6. Por el teorema de Galois, debe haber tres cuerpos intermedios propios entre $\mathbb{Q}$ y $\mathbb{Q}(\alpha)$, y se corresponden con $F(H_2), F(H_3), F(H_4)$.

- $\mathbb{Q}[i] = \mathbb{Q}[\alpha^2]$ porque $\alpha^2 = i$. Como $\alpha^2 = x_2$, por el apartado 4 vemos que $\sigma_3(x_2) = x_2$, de donde $\mathbb{Q}[\alpha^2) \subset F(H_3)$. Además, $[\mathbb{Q}[i] : \mathbb{Q}] = 2$ y $[F(H_3) : \mathbb{Q}] = \frac{4}{2} = 2$, con lo que tenemos $\mathbb{Q}[i] = F(H_3)$. El caso d) es igual.
- Un razonamiento análogo al anterior nos dice que $[F(H_i) : \mathbb{Q}] = 2, i = 2, 3, 4$. De $\alpha = \frac{1}{2}(1+i)\sqrt{2}$ deducimos que $\sqrt{2} = \frac{2\alpha}{1+\alpha^2} \in K$. Entonces $\mathbb{Q}[\sqrt{2} \subset K$ y es un cuerpo intermedio, distinto del anterior. Veamos si es $F(H_2)$ o $F(H_4)$. Tenemos que

$$\sigma_2(\sqrt{2}) = \sigma_2(\frac{2\alpha}{1+\alpha^2}) = \frac{2\alpha^3}{1+\alpha^6} = \sqrt{2}\,\frac{-1+i}{1-i} = -\sqrt{2} \neq \sqrt{2}.$$

Por tanto, el elemento $\sqrt{2}$ no permanece invariante por σ_2, de donde $\mathbb{Q}[\sqrt{2}] = F(H_4)$.
- Es claro que $\sqrt{-2} = \sqrt{2}i$ por lo que $\sqrt{-2} \in K$ y $\mathbb{Q}[\sqrt{-2}] \subset K$. Como $[\mathbb{Q}[\sqrt{-2} : \mathbb{Q}] = 2$, es el otro cuerpo intermedio: $\mathbb{Q}[\sqrt{-2}] = F(H_2)$.
- Ya sabemos que $\alpha + \alpha^2 \in K$, de donde $\mathbb{Q}[\alpha + \alpha^2]$ es un cuerpo intermedio.
- Como $\mathbb{Q}[\sqrt{3}] \neq \mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{-2}], \mathbb{Q}[i]$ y $\mathbb{Q}[\sqrt{3} : \mathbb{Q}] = 2$, no es un cuerpo intermedio (solamente hay tres).

Ejercicio 3. (*1 punto*) Sea G un grupo finito de orden impar y $x \in G$. Demuestre que existe $y \in G$ tal que $x = y^2$.

Solución. Sea $x \in G$. Si $|G| = 2n+1$, entonces $x^{2n+1} = 1$, de donde $x = x^{-2n} = (x^{-n})^2$. Tomamos $y = x^{-n}$, y tenemos el resultado.

Ejercicio 4. (*1 punto*) Sea H un subgrupo normal de orden dos de un grupo G. Pruebe que $H \subset C(G)$.

Solución. Como H es de orden 2, podemos escribir $H = \{1, h\}$, con $h \neq 1$. Recordemos que $C(G) = \{g \in G | ag = ga \text{ para todo } a \in G\}$. Es claro que $1 \in C(G)$. Veamos qué ocurre con el elemento h. Sea $a \in G$ un elemento cualquiera. Como H es subgrupo normal de G, tenemos que $aha^{-1} \in H$. Tenemos dos posibilidades:

- Si $aha^{-1} = 1$ entonces $h = a^{-1}a = 1$, lo que no es posible.
- Si $aha^{-1} = h$ entonces $ah = ha$, que es lo que queríamos probar.

Ejercicio 5. (*1 punto*) Consideremos en S_7 la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 7 & 4 & 6 & 2 & 3 \end{pmatrix}.$$

Calcule la descomposición en ciclos disjuntos de $\sigma, \sigma^2, \sigma^{-1}$. Calcule el orden de $\sigma, \sigma^2, \sigma^{-1}$.

Solución. La descomposición en ciclos disjuntos de σ es $(256)(37)$. Entonces $\sigma^2 = (256)(37)(256)(37) = (256)(256) = (265)$, porque ciclos disjuntos conmutan. Análogamente, $\sigma^{-1} = (37)^{-1}(256)^{-1} = (37)(265)$. Como el orden del ciclo (256) es 3, y el de (37) es 2, el orden de σ es $\text{mcm}(2,3) = 6$. El orden de σ^2 es 3, y el orden de σ^{-1} es el mismo que el de σ, esto es, vale 6.

Cuestión 1. (*1,5 puntos*).

1. Definición de subgrupo normal.
2. Definición de extensión normal de un cuerpo.
3. Relación entre ambos conceptos.

Solución. Para las dos primeras, consulte la teoría. La tercera se refiere al teorema fundamental de la teoría de Galois. Sea $f(X) \in k[X]$ un polinomio separable, K cuerpos de descomposición de $f(X)$ sobre k y G el grupo de Galois de $f(X)$ sobre k. Entonces un subgrupo H de G es normal si y solamente si $F(H)|k$ es una extensión normal, y en tal caso, $\text{Gal}(F(H)|k) \simeq G/H$.